

### REMARKS

Response is hereby made to the Office Action dated December 18, 2003. By this Response, Applicant has amended claim 1 without prejudice or disclaimer, and claims 1-18 remain pending the application. *Although no fee or extension of time is believed to be required by this Response, the Commissioner is authorized and requested provide any extensions of time and/or to debit any fees that may be required by this Response (including any fees for additional claims or extensions of time) from Deposit Account No. 50-2091 to avoid abandonment of this Application.*

The Office Action rejects each of the claims under 35 USC § 103, citing various combinations of US Patent No. 6,253,324 ("Field") and US Patent No. 5,822,432 ("Moskowitz"). Applicant respectfully traverses the rejections in that neither reference fails to disclose or suggest each and every element of the claims, taken singly or in combination. For example, no reference of record discloses at least the step of *randomly determining position information indicative of a position within a data stream to be generated within the remote unit at which said random value is to be located*, as recited in claim 1.

As stated in Applicant's previous response, the present claims recite methods and devices for identifying tampering in a remote device such as a cable television box or the like. The method recited in claim 1 involves producing three random data values (a random number, a memory range, and a position in the data stream for storing the random number) and providing each of these data values to the remote device for processing. Security, then, is provided by three randomly generated variables: the random number key, the hashed memory range of the remote device, and the location in the data stream.

The primary reference, Field, expressly relates to a client/server system wherein both the client and the server execute concurrently on a single computer (see Field col. 6, lines 17-24, emphasis added). The reference therefore relates solely to interprocess communications within a single device; it does not relate to verifying the integrity of a remote unit in a communication system in any way. The Field reference therefore cannot disclose at least *randomly determining position information indicative of a position within a data stream to be generated within the remote unit*, as correctly noted by the Examiner, since the reference does not include a data

stream or a remote unit as recited by the present claims. Further, Applicant has amended claim 1 to now recite that the range of memory space within the remote unit having data to be hashed is randomly determined. Even to the extent that Fields does disclose a range of memory space to be hashed, this range is not determined randomly. The Fields reference therefore does not anticipate Applicant's claims on its own merits.

Even when the Fields reference is combined with the Moskowitz reference, however, the combination of the two still fails to describe each and every aspect of Applicant's claims. Indeed, Moskowitz does not relate to verifying the integrity of a remote unit in any way, but rather clearly relates to a system of watermarking a digital bitstream such as an audio/visual file. This watermark is essentially a digital code that is combined with the bitstream itself (see Moskowitz col. 1, lines 16-18 and 37-41) when the bitstream is created. Moreover, the watermarks disclosed in the Moskowitz reference are clearly described as having parameters that are determined by a human engineer (see, e.g., Abstract lines 5-7 and col. 5, lines 50-55). Accordingly, Moskowitz does not "randomly determine" the various parameters as recited in claim 1. Further, Moskowitz has no need for the "position information" recited in Applicant's claims, since Moskowitz is in no way concerned with determining a data stream to be generated within the remote unit. Indeed, the language cited in the Office Action as allegedly disclosing this element (col. 3, lines 24-30) simply relate to "a randomly generated sequence of binary zeros and ones" that make up the watermark. This language in no way anticipates any aspect of position in a data stream or of any other data generated by a remote unit. Therefore, neither Fields nor Moskowitz (nor the combination of the two) disclose each and every limitation of Applicant's claims.

Further, because each of the dependent claims inherits the restrictions of its parent independent claim, the dependent claims are believed to be patentable *a fortiori*, and a detailed analysis of the patentability of these claims is not required at this time. Nevertheless, Applicant does not consent to any of the rejections found in the Office Action, and expressly reserves the right to separately dispute the patentability of any dependent claim at a later date, if necessary to do so.

Applicant has addressed each of the concerns set forth in the Office Action, and all of the pending claims are therefore believed to be allowable. Applicant therefore respectfully

requests reconsideration and withdrawal the rejections set forth in the Office Action, and allowance of each of the remaining claims. Should the Examiner have any questions or wish to further discuss this application, Applicant requests that the Examiner contact the undersigned at (480) 385-5060 or bcarlson@ifllaw.com.

Dated

8/31/2004

Respectfully submitted,



Brett A. Carlson

Reg. No. 39,928

**Ingrassia Fisher & Lorenz P.C.**  
Customer No. 29906